IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

22-CR-6009-CJS-MJP

JOHN DOUGLAS LOONEY,

Defendant.

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTIONS

The United States of America, by and through its attorneys, Trini E. Ross, United States Attorney for the Western District of New York, and Meghan K. McGuire, Assistant United States Attorney, hereby responds to defendant's supplemental motion to suppress (Dkt. 72).

FACTUAL BACKGROUND

In 2018 and 2019, Federal Bureau of Investigations ("FBI") Task Force Officer ("Ofc.") Carlton Turner was investigating the illegal exchange of child pornography on a particular peer-to-peer file sharing network (hereinafter the "Network"). On three separate occasions, Ofc. Turner observed requests for child pornography files coming from an IP address that was registered to the defendant's residence.

Based on these requests and the defendant's prior conviction, Ofc. Turner sought and obtained a warrant from the Hon. Marian W. Payson to search the defendant's residence for evidence of the possession and distribution of child pornography.

In Ofc. Turner's supporting affidavit, he explained that, in the Network's "opennet" mode, users could see the IP addresses of their peers:

> 23. The particular P2P network has two operational modes, "Darknet" and "Opennet." On the Darknet mode, a computer connects only to peers whom the user has specifically selected. On the Opennet mode, a computer may connect to peers unknown to the user. A user may choose which mode to use. The mode relevant to this investigation involves a user who chose to use the Opennet operational mode.
>
> 24. The Network warns its users in multiple ways that it does not guarantee anonymity: when the software is initially installed; within the log file each time the Network is started; and via the Network's publicly accessible website. The Network's software also does not mask a computer's IP address — the IP addresses of each user's peers are observable to the user. For example, if a user is connected to 10 peers on the P2P network, all 10 of those peers' IP addresses will be observable to the user. The fact that the Network does not mask IP addresses is explained on its publicly accessible website. The Network also acknowledges on its publicly accessible website that, for users who use the Opennet mode, it can be statistically shown that a particular user more likely than not requested a file (as opposed to having merely forwarded the request of another peer) based on factors including the proportion of the pieces of a file requested by a user and the number of nearby peers.

Ofc. Turner's affidavit also explained that law enforcement conducted undercover investigations on the Network using a modified version of the Network software. The modification allowed law enforcement to record information that is available to all Network users, as explained in the following paragraphs of Ofc. Turner's affidavit:

> 32. The information logged by law enforcement version is nearly identical to the original Network, except that it allows a computer operated by a law enforcement officer to automatically log information about requests received directly from its peers. The types of information logged by a law enforcement computer are available to all standard Network users as part of the Network's normal operation.
>
> 33. The information logged by law enforcement includes, but is not limited to: the IP addresses of the law enforcement computer's peers; the number of peers those peers report to have; a unique identifier assigned by the software (referred to as the computer's Network "location"); the remaining

> number of times a request for a piece of a file may be forwarded; the date/time of requests received from a peer; and the digital hash value of a requested piece.
>
> 34. Law enforcement computers do not target specific peers on the Network and law enforcement computers do not solicit requests from any peers. They simply record requests for blocks of files known to contain child pornography made by peers.

As Ofc. Turner explained, the modified version of the Network software only gave law enforcement information—including the IP addresses of a peer computer and the digital hash value of a requested piece—that all users of the Network had access to. It did not provide law enforcement with any additional information that was not available to other, non-law enforcement users.

On March 1, 2019, the FBI executed the warrant at the defendant's residence. While executing the search warrant, the FBI found three laptops. In total, these laptops contained over 1 million images and videos of child pornography. The FBI also found a pair of thumb drives that contained a folder named after the Network. The Network folder contained approximately 300 manifest keys for child pornography files.

On January 18, 2022, a federal grand jury returned a three-count Indictment against the defendant, charging him with possessing child pornography, in violation of Title 18, United States Code, Section 2252A(a)(5)(B) and (b)(2). (Dkt. 36.)

On February 4, 2022, the government filed its Notice of Intent to Use Evidence (Dkt. 41) advising the defendant of its intent to offer the items seized during the execution of the search warrant—including the three laptops that contained over 1,000,000 child pornography files and the two thumb drives that contained child pornography manifest keys—as evidence

at trial. On February 24, 2023, the defendant filed a motion to suppress this evidence. (Dkt. 72.)

DISCUSSION

A. THE DEFENDANT DID NOT HAVE A REASONABLE EXPECTATION OF PRIVACY IN THE IP ADDRESS AND HASH VALUES OFC. TURNER OBSERVED

The Fourth Amendment protects "against unreasonable searches and seizures." U.S. Const. Amend. IV. A Fourth Amendment analysis begins with analyzing whether the defendant possessed a reasonable expectation of privacy in the object being searched. *Katz v. United States*, 389 U.S. 347, 353 (1967). The burden of showing a legitimate expectation of privacy in the area searched rests with the defendant. *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980). The Supreme Court has repeatedly explained, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection").

When a user on a peer-to-peer file sharing network (like the Network at issue in this case) requests a file from his peers, the requestor is voluntarily turning over information—including the requestor's IP address and the hash value of the file being requested—to those peers. As such, "the federal courts of appeals that have examined the privacy implications of searching peer-to-peer networks for files potentially containing child pornography have concluded that a search of publicly available information does not violate a computer user's reasonable expectation of privacy." *United States v. Thomas*, No. 5:12-CR-37, 2013 WL 6000484, at *19 (D. Vt. Nov. 8, 2013), *aff'd*, 788 F.3d 345 (2d Cir. 2015) (*citing United States v.*

Norman, 448 F. App'x 895 (11th Cir. 2011) (search of defendant's computer did not constitute an unlawful search because information on shared folder was also available to members of the public); *United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir. 2010) (rejecting the argument that the defendant had a reasonable expectation of privacy in files that were shared on a peer-to-peer file sharing site, regardless of defendant's intent to maintain the files as private); *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009) (defendant had no reasonable expectation of privacy in files that the FBI retrieved from his personal computer where the peer-to-peer program the defendant used made files accessible to other users); *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008) (defendant had no expectation of privacy in his subscriber information because peer-to-peer software permitted anyone else on the Internet to access at least certain folders in his computer and such access could expose his subscriber information to outsiders).

To the government's knowledge, every court that has considered the question of whether a requestor on the Network has a reasonable expectation of privacy in the IP address and hash value information that is transmitted with their request has found that they do not. *See United States v. Pobre*, No. 8:19-CR-348-PX, 2022 WL 1136891, at *7 (D. Md. Apr. 15, 2022) ("Pobre has not convinced this Court that his [Network] activities are protected by the Fourth Amendment. The [law enforcement node] captures only that information which Pobre has willingly disclosed to third parties in opennet mode. Nor is there anything particularly sophisticated about law enforcement's software—it simply permits the law enforcement node access to information otherwise available to others in the [Network] space."); *United States v. Sigouin*, 494 F. Supp. 3d 1252, 1264 (S.D. Fla. 2019) ("[T]ransmitting the hash value via the Network is the equivalent of loudly asking for something in a room full of strangers. There is

no objectively reasonable expectation of privacy."); *United States v. Dickerman*, No. 416CR00258HEANAB1, 2017 WL 11485604, at *13 (E.D. Mo. Sept. 26, 2017), *report and recommendation adopted*, No. 4:16CR258 HEA, 2018 WL 10228437 (E.D. Mo. Apr. 27, 2018), *aff'd*, 954 F.3d 1060 (8th Cir. 2020) ("The Government argues persuasively that this case is substantially analogous to the origins of the third party doctrine, namely, that an otherwise voluntary exchange with undercover government agents and the recording thereof is not protected by the Fourth Amendment. . . . Dickerman knowingly downloaded an application that networked his computer with those of complete strangers for the purpose of sharing files. In doing so, he assumed the risk that one of his associates would be less than trustworthy."); *United States v. Hall*, 16-CR-469 (D.Md. Aug. 30, 2017) (oral order denying motion to suppress evidence found pursuant to search warrant that was based on information obtained from the defendant's Network requests and rejecting argument defendant had a reasonable expectation of privacy in that information); *United States v. Hebert*, 16-CR-0104, Dkt. 57 (D. Wy. Oct. 7, 2016) (same).

The defendant's motion implies that the information Ofc. Turner observed was not generally available to non-law enforcement users on the Network. (Def. Mot., Dkt. 72, p. 6.) That is factually inaccurate. Ofc. Turner explained in his affidavit that, "[t]he types of information logged by a law enforcement computer are available to all standard Network users as part of the Network's normal operation." (Turner Aff., ¶ 32.)

As such, the defendant has failed to meet his burden of demonstrating that he had a reasonable expectation of privacy in the information he shared when he requested files from Ofc. Turner on the Network. Because there was no expectation of privacy in the requests,

law enforcement did not conduct a search when they observed and recorded the information that the defendant voluntarily disclosed. The defendant therefore cannot invoke the protections of the Fourth Amendment.

B. THE ELECTRONIC COMMUNICATIONS ACT DOES NOT APPLY

The Electronic Communications Privacy Act ("ECPA") prohibits "intentionally intercept[ing] ... any wire, oral, or electronic communication," unless the intercept is authorized by court order. 18 U.S.C. § 2511(1)(a). One exception to the SCA states, "it shall not be unlawful [] for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communications has given prior consent to such interception." 18 U.S.C. § 2511(2)(c). This exception permits undercover law enforcement officers and confidential informants to engage in consensual wire communications with a target without obtaining a warrant. *See United States v. Johnson*, 762 F. App'x 21, 23 (2d Cir. 2019) (warrantless electronic monitoring and recording of communications with the consent of one party is not a violation of Title III).

Defendant's motion argues that Ofc. Turner's observation of the IP address and hash value information violated the ECPA. This argument is completely off base because Ofc. Turner was a party to the exchanges. He was acting in an undercover capacity on the Network and connected to the defendant's computer as a peer. The defendant sent requests for child pornography files—which requests included the defendant's IP address and hash value information— to all his peers, including Ofc. Turner. Ofc. Turner was a party to this voluntary communication. Thus, the exception under 18 U.S.C. § 2511(2)(c) applies.

The defendant has also failed to establish that the information Ofc. Turner collected constituted a "wire, oral, or electronic communication," as defined by the statute. Rather, the information is more akin to record information. *See In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014) ("[U]nder ECPA, the term 'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication.")

Because Ofc. Turner was a party to the defendant's requests and the defendant has failed to establish that those requests constituted communications, the ECPA is wholly inapplicable to this case.

C. THE STORED COMMUNICATIONS ACT DOES NOT APPLY

The Stored Communications Act prohibits "intentionally access[ing] without authorization a facility through which an electronic communication service is provided . . . and thereby obtain[ing] . . . a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701.

The SCA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. §§ 2711(1) and 2510(17).

The SCA also contains an exception for "a user of [a wire electronic communications] service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c)(2).

The defendant argues that Ofc. Turner's receipt of the defendant's requests for child pornography files violated the SCA. This argument fails for several reasons. First, the defendant has not established that the Network meets the definitions of a "facility through which an electronic communication service is provided." Second, he has not established that his requests constitute "communications." Third, even if the requests constituted communications, they were not stored communications; they were active requests directed at Ofc. Turner. Fourth, the defendant voluntarily transmitted his requests to all his peers, including Ofc. Turner. As such, the exception under 18 U.S.C. § 2701(c)(2) applies.

The defendant also argues that law enforcement violated the SCA by obtaining the subscriber information associated with his IP address via a subpoena. (Def. Mot., Dkt. 72, p. 11.) However, 18 U.S.C. § 2703(c)(2) expressly permits law enforcement to obtain subscriber information from an electronic commination service or remote computing service provider with a subpoena.

Moreover, even if law enforcement had violated the SCA in by receiving the defendant's requests, suppression is not an appropriate remedy. The exclusive remedy for a violation of the SCA is a civil action for damages and criminal punishment under certain circumstances, not suppression of evidence. See 18 U.S.C. § 2708 ("The [damages] remedies and sanctions described in this chapter are the only judicial remedies and sanctions for non-constitutional violations of this chapter."). Accordingly, non-constitutional violations[1] of the SCA do not result in suppression of the evidence. *See United States v. Kornaker*, No. 21-CR-

[1] As is set forth in Section A, above, the defendant did not have a reasonable expectation of privacy in the information associated with his Network requests and therefore there is no constitutional violation of the SCA.

37A, 2021 WL 7500251, at *5 (W.D.N.Y. Oct. 22, 2021), *report and recommendation adopted*, No. 21-CR-37A, 2022 WL 787965 (W.D.N.Y. Mar. 15, 2022) ("Even if there were a violation of the Stored Communications Act, suppression of evidence is not an available remedy.").

D. THE PEN REGISTER ACT DOES NOT APPLY

The Pen Register and Trap and Trace Statute ("Pen Register Act") states that "no person may install or use a pen register or a trap and trace device without first obtaining a court order." 18 U.S.C. § 3121. "The term 'pen' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3)

The defendant argues that Ofc. Turner violated 18 U.S.C. § 3121 because the defendant's IP address constituted "routing information." But Ofc. Turner's affidavit clearly establishes that he did not obtain "routing information." Rather, he obtained the IP address of the computer from which he received a request. A single IP address that is voluntarily transmitted from one computer to another is not covered by the Pen Register Statute. *See Capitol Recs. Inc. v. Thomas-Rasset*, No. CIV 06-1497(MJD/RLE), 2009 WL 1664468, at *3 (D. Minn. June 11, 2009) (["T]he Pen Register Act cannot be intended to prevent individuals who receive electronic communications from recording the IP information sent to them. If it did apply in those cases, then the Internet could not function because standard computer operations require recording IP addresses so parties can communicate with one another over the Internet.").

Moreover, as with the SCA, the exclusive remedy for non-constitutional violations of the Pen Register Act are civil actions and criminal charges. 18 U.S.C. §§ 3121(d) and 2707(g). Suppression is not an available remedy.

E. THE GOOD FAITH EXCEPTION TO THE EXCLUSIONARY RULE APPLIES IN THIS CASE

"The exclusionary rule is a judicially created doctrine that is prudential rather than constitutionally mandated. It therefore applies only where its deterrence benefits outweigh its substantial social costs. The extent to which the exclusionary rule is justified by deterrence principles varies with the culpability of the law enforcement conduct." *United States v. Jones*, 43 F.4th at 110 (quotations omitted).

"Because the exclusionary rule exacts a heavy toll on the justice system, it applies only to deter law enforcement's deliberate, reckless, or grossly negligent conduct." *Id.* (quotations omitted). "In accord with these principles, the 'good-faith exception' to the exclusionary rule applies when the agents . . . act with an objectively reasonable good-faith belief that their conduct is lawful." *Id.* (quotation omitted).

For the reasons discussed above, Ofc. Turner clearly acted in good faith when, while operating in a undercover capacity on the Network, he received the requests for child pornography files from the defendant and the information associated with those requests. Because there is no evidence of bad faith on Ofc. Turner's part, the Court can and should deny the defendant's motion on this ground alone.

Dated: Rochester, New York
March 14, 2023

TRINI E. ROSS
United States Attorney

By: *s/Meghan K. McGuire*

MEGHAN K. MCGUIRE
Assistant United States Attorney
U.S. Attorney's Office
100 State Street, Suite 500
Rochester, NY 14614
(585) 399-3922
Meghan.McGuire@usdoj.gov